

The Honorable Kymberly K. Evanson

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN FLOYD, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

AMAZON.COM, INC., a Delaware corporation,
and APPLE INC., a California corporation,

Defendants.

No. 2:22-cv-01599-KKE

**PROTOCOL REGARDING
DISCOVERY OF ELECTRONICALLY
STORED INFORMATION AND
ORDER**

A. General Principles

1. An attorney's zealous representation of a client is not compromised by conducting discovery in a cooperative manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions.

2. As provided in LCR 26(f), the proportionality standard set forth in Fed. R. Civ. P. 26(b)(1) must be applied in each case when formulating a discovery plan. To further the application of the proportionality standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as possible. When a party propounds discovery requests pursuant to Fed. R. Civ. P. 34, the parties agree to meet and confer regarding the phasing and prioritization of productions.

3. This Order may be modified by a Stipulated Order of the parties or by the Court

for good cause shown. Any such modified Order will be titled sequentially as follows, “First Modified Order re: Discovery of Electronically Stored Information for Standard Litigation,” and each modified Order will supersede the previous Order.

4. Nothing in this Order precludes the parties from reaching further agreements on topics related to this Order, or if agreement cannot be reached, moving the Court for an appropriate discovery order.

B. ESI Disclosures

Within 60 days of any party’s first substantive responses to discovery requests, or at a later time if agreed to by the parties, each party shall disclose:

1. Custodians. The custodians most likely to have discoverable ESI in their possession, custody, or control. The custodians shall be identified by name, title, connection to the instant litigation, and the type of the information under the custodian’s control. The parties shall meet and confer to reach agreement on a reasonable list of custodians for purposes of collection, review and production of electronically stored information.

2. Non-custodial Data Sources. A list of non-custodial data sources (*e.g.*, shared drives, servers), if any, likely to contain discoverable ESI.

3. Third-Party Data Sources. A list of third-party data sources, if any, likely to contain discoverable ESI (*e.g.*, third-party email providers, mobile device providers, cloud storage) and, for each such source, the extent to which a party is (or is not) able to preserve information stored in the third-party data source.

4. Inaccessible Data. A list of data sources, if any, likely to contain discoverable ESI (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the data source) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

5. Foreign data privacy laws. Nothing in this Order is intended to prevent either party from complying with the requirements of a foreign country’s data privacy laws, *e.g.*, the European Union’s General Data Protection Regulation (GDPR) (EU) 2016/679. The parties agree to meet

1 and confer before including custodians or data sources subject to such laws in any ESI or other
2 discovery request.

3 **C. ESI Discovery Procedures**

4 1. On-site inspection of electronic media. Such an inspection shall not be required
5 absent a demonstration by the requesting party of specific need and good cause or by agreement
6 of the parties.

7 2. Search methodology. The parties shall timely confer to attempt to reach agreement
8 on appropriate search terms and queries, file type and date restrictions, data sources (including
9 custodians), and other appropriate computer- or technology-aided methodologies, before any such
10 effort is undertaken. The parties shall continue to cooperate in revising the appropriateness of the
11 search methodology.

12 a. Prior to running searches:

13 i. The producing party shall disclose the data sources (including
14 custodians), search terms and queries, any file type and date restrictions, and any other
15 methodology that it proposes to use to locate ESI likely to contain responsive and discoverable
16 information. The requesting party may request, and the producing party may provide, unique hit
17 counts for each search query. To the extent any disputes arise regarding the provision of hit
18 counts, the parties shall meet and confer in a good-faith effort to resolve the issue.

19 ii. After disclosure, the parties will engage in a meet and confer
20 process regarding additional terms sought by the non-producing party.

21 iii. The following provisions apply to search terms/queries of the
22 requesting party. Focused terms and queries should be employed; broad terms or queries, such as
23 product and company names, generally should be avoided. A conjunctive combination of multiple
24 words or phrases (*e.g.*, “computer” and “system”) narrows the search and shall count as a single
25 search term. A disjunctive combination of multiple words or phrases (*e.g.*, “computer” or
26 “system”) broadens the search, and thus each word or phrase shall count as a separate search term
27 unless they are variants of the same word. The producing party may identify each search term or

query returning overbroad results demonstrating the overbroad results and a counterproposal correcting the overbroad search or query. The parties will meet and confer to address concerns relating to overbroad search term results.

3. Format.¹

a. ESI will be produced to the requesting party with searchable text to the extent it exists, in a format to be decided between the parties. The producing party shall include the files specified in Exhibit A with each production, to the extent they are reasonably accessible and non-privileged.

b. Unless otherwise agreed to by the parties, files that are not easily converted to image format, including but not limited to spreadsheet, database, audio, video, and drawing files, will be produced in native format.

c. Each document image file shall be named with a unique number (Bates Number). Documents produced in native format will be assigned a Bates Number and be produced with a corresponding load file. File names should not be more than twenty characters long or contain spaces.

d. If a document is more than one page, the unitization of the document and any attachments and/or affixed notes shall be maintained as they existed in the original document.

e. The full text of each electronic document shall be extracted (“Extracted Text”) and produced in a text file. The Extracted Text shall be provided in searchable ASCII text format (or Unicode text format if the text is in a foreign language) and shall be named with a unique Bates Number (*e.g.*, the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension).

¹ Documents that are not produced in the first instance in this litigation, i.e., documents that were previously produced in other matters, shall be produced pursuant to the ESI protocols governing the format of document productions in those other matters, provided that those re-productions are in a reasonably useful format and provided that the producing party informs all other parties, prior to or at the time of production, that the production will be in a nonconforming format. The parties reserve the right to object to a nonconforming format.

1 4. De-duplication. The parties may de-duplicate their ESI production across custodial
2 and non-custodial data sources after disclosure to the requesting party, and the duplicate custodian
3 information removed during the de-duplication process shall be tracked in a custodian field in the
4 database load file. If processing and production is done on a rolling basis, an updated duplicate
5 custodian field with additional values shall be provided in an overlay. The producing party shall
6 identify whether the overlay replaces previously produced fields for a file or supplements them.

7 5. Email Threading. The parties may use analytics technology to identify email
8 threads and need only produce the unique most inclusive copy and related family members and
9 may exclude lesser inclusive copies. Upon reasonable request, the producing party will produce
10 a less inclusive copy or missing metadata, if, for example, a threaded email cuts off
11 to/from/cc/subject line/date information.

12 6. Metadata fields. If the requesting party seeks metadata, the parties agree that only
13 the metadata fields identified in Exhibit B need be produced, and only to the extent they are
14 reasonably accessible and non-privileged. The list of metadata included in Exhibit B is intended
15 to be flexible and may be changed by agreement of the parties.

16 7. Databases. Certain types of databases are dynamic in nature and may contain
17 information that is neither relevant nor reasonably calculated to lead to the discovery of
18 admissible evidence. The parties shall meet and confer regarding whether such databases must
19 be produced and the appropriate format for productions from dynamic databases, including as to
20 whether the data may be produced in an alternate form, such as a report, data table, or other
21 static format. The parties agree to identify the specific databases, by name, that contain the
22 relevant and responsive information that parties produce.

23 8. Hard-Copy Documents. If the parties elect to produce hard-copy documents in an
24 electronic format, the production of hard-copy documents will include a cross-reference file that
25 indicates document breaks and sets forth the custodian or custodian/location associated with each
26 produced document. Hard-copy documents will be scanned using Optical Character Recognition
27 technology and searchable ASCII text files will be produced (or Unicode text format if the text is

in a foreign language), unless the producing party can show that the cost would outweigh the usefulness of scanning (for example, when the condition of the paper is not conducive to scanning and will not result in accurate or reasonably useable/searchable ESI). Each file will be named with a unique Bates Number (*e.g.*, the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension).

D. Preservation of ESI

The parties acknowledge that they have a common law obligation, as expressed in Fed. R. Civ. P. 37(e), to take reasonable and proportional steps to preserve relevant and discoverable information in the party's possession, custody, or control. With respect to preservation of ESI, the parties agree as follows:

1. Absent a showing of good cause by the requesting party, the parties shall not be required to modify the procedures used by them in the ordinary course of business to back up and archive data; provided, however, that the parties shall preserve all discoverable ESI in their possession, custody, or control.

2. The parties will supplement their initial disclosures in accordance with Fed. R. Civ. P. 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosures where that data is created after a disclosure or response is made (unless excluded under Sections D(3) or E(1)-(2)). The parties will meet and confer in good faith regarding a reasonable schedule and cut-off date for supplementation.

3. Only unique, non-duplicative sources of relevant documents need to be preserved. The parties shall use objective measures to determine whether two sources are duplicative. Where documents are possessed by multiple custodians, each custodian's copy is a unique, non-duplicative document.

4. Absent a showing of good cause by the requesting party, the following categories of ESI that need not be preserved include:

a. Deleted, slack, fragmented, or other data only accessible by forensics.

- b. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.
- c. On-line access data such as temporary internet files, history, cache, cookies, and the like.
- d. Interim automatically saved drafts, as opposed to drafts saved by a user.
- e. Data in metadata fields that are frequently updated automatically, such as last-opened dates (see also Section (E)(5)).
- f. Dynamic fields of databases or log files that are not retained in the usual course of business.
- g. Back-up data that are duplicative of data that are more accessible elsewhere.
- h. Server, system or network logs.
- i. Data remaining from systems no longer in use that is unintelligible on the systems in use.
- j. Electronic data (*e.g.*, email, calendars, contact data, and notes) sent to or from mobile devices (*e.g.*, iPhone, iPad, Android devices), provided that a copy of all such electronic data is automatically saved in real time elsewhere (such as on a server, laptop, desktop computer, or “cloud” storage).

5. The parties agree to confer in good faith regarding adding other categories to this list.

E. Privilege

1. The parties agree to abide by Fed. R. Civ. P. 26(b)(5) with respect to documents fully withheld from production on the basis of a privilege or other protection, unless otherwise agreed or excepted by this Agreement or Order. Privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged or work-product protection). For ESI, the privilege log may be generated using available metadata, including

author/recipient or to/from/cc/bcc names; the subject matter or title; and date created. Should the available metadata provide insufficient information for the purpose of evaluating the privilege claim asserted, the producing party shall include such additional information as required by the Federal Rules of Civil Procedure. Privilege logs will be produced no later than 60 days after the deadline for substantial completion of document productions. To the extent a party produces documents after the deadline for substantial completion, and withholds from such production any documents on the basis of privilege, that party shall provide a supplemental privilege log within 30 days of the production. A document initially included on a privilege log may be produced after the close of fact discovery, either by agreement or when the basis for the privilege asserted has been successfully challenged by another party.

2. Redactions need not be logged so long as the basis for the redaction is clear on the redacted document.

3. With respect to privileged or work-product information generated after the filing of the complaint, parties are not required to include any such information in privilege logs.

4. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).

5. Pursuant to Federal Rule of Evidence 502(d) and (e), the production of a privileged or work product protected document is not a waiver of privilege or protection from discovery in this case or in any other federal or state proceeding. For example, the mere production of a privileged or work product protected document in this case as part of a production is not itself a waiver. Nothing in this Order shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work product doctrine, or any other applicable privilege or immunity. The parties do not waive any objections as to the production, discoverability, admissibility, or confidentiality of documents and ESI. Moreover, nothing in this Order shall be interpreted to require disclosure of information subject to privacy protections as set forth in law or regulation, including information that may need to be produced from outside of the United States and/or may be subject to foreign laws.

F. Non-Party Discovery

1. A party that issues a non-party subpoena (the “Issuing Party”) shall include a copy of this ESI Protocol with the subpoena.

2. The Issuing Party shall be responsible for producing any documents obtained under a subpoena to all other parties.

3. If the non-party production is not Bates-stamped, the Issuing Party shall endorse the non-party production with unique prefixes and Bates numbers prior to producing them to all other parties.

G. Foreign-Language Documents

All documents shall be produced in their original language. Where a requested document exists in a foreign language and the producing party also has an English-language version of that document that it prepared for non-litigation purposes prior to filing of the lawsuit, the producing party shall produce both the original document and all English-language versions. In addition, if the producing party has a certified translation of a foreign-language document that is being produced (whether or not the translation is prepared for purposes of litigation), the producing party shall produce both the original document and the certified translation. Nothing in this Agreement shall require a producing party to prepare a translation, certified or otherwise, for foreign-language documents that are produced in discovery.

EXHIBIT A – FILE STRUCTURE

File Structure. The Producing Party shall produce the following sets of files with each production.

a. Image Load File.

- (1) Every document referenced in a production image load file must have all corresponding images, text and metadata.
- (2) The name of the image load file must mirror the name of the delivery volume and should have an .OPT file extension.
- (3) The volume names must be reasonably consecutive (e.g. ABC001, ABC002...).
- (4) The load file must contain one line per image.
- (5) Every image in the delivery volume must be contained in the image load file.
- (6) The image key must be named the same as the Bates number of the image.
- (7) Load files must not span across media.
- (8) File should be placed in the root directory or a directory labeled "DATA."

b. Metadata Load File.

- (1) Each production has one load file, in "Concordance" style .DAT format.
- (2) Values must be enclosed by þ (ASCII Decimal 254).
- (3) Values must be separated by the "Device Control 4" character, ASCII decimal 20.
- (4) First line must contain the column/field names (set forth in Section IV, below).
- (5) The fields Begin Bates and End Bates must be present, and the first fields listed in the load file.
- (6) The field NativePath must be present if native files are included in the document production.
- (7) Each subsequent row must contain the Metadata for one

Document.

- (8) Every row must have the same number of columns/fields (empty values are acceptable).
- (9) Text must be encoded in UTF-8.
- (10) File should be placed in the root directory or a directory labeled "DATA."

c. OCR and Extracted Text Files (.TXT Files).

- (1) A single text file for each Document containing all the Document's pages, in text.
- (2) Pages separated by form feed character (decimal 12, hex 0xC).
- (3) Filenames should be of the form: <Bates num>.txt, where <Bates num> is the Bates number of the first page of the Document.
- (4) Text must be encoded in UTF-8.
- (5) Files should be placed in a directory labeled "TEXT."

d. Image Files.

- (1) Document level PDF, slipsheet image, or Single-page Group IV TIFF images for each Document, containing all images for that document.
- (2) Filenames should be of the form: <Bates num>.<ext>, where <Bates num> is the BATES number of the first page of the document (i.e., the "Begin Bates" number), and <ext> is the appropriate extension for the image format (.pdf or .tiff).
- (3) Files should be placed in the "IMAGES" subdirectory.

e. Native Files.

- (1) Document level native file for each native file included in the document production.
- (2) Filenames should be of the form: <Bates num>.<ext>, where <Bates num> is the BATES number of the document. Confidentiality designations may be included in the filenames, after the BATES number.
- (3) A relative link to the location of the native file in the document

1 productions shall be produced in NATIVEPATH metadata field in
2 the .DAT load file.

3 (4) Files should be placed in a directory named "NATIVES."
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

EXHIBIT B - METADATA FIELDS

For ESI and documents that were originally stored in electronic format, all fields below should be provided, to the extent reasonably available. Applicable fields will be provided for scanned hard copy documents. The parties acknowledge that not all fields below may be reasonably available to all producing parties, and further that a producing party does not violate this Order by failing to include in its productions metadata fields that are not reasonably available. Unless otherwise agreed by the parties, the field-naming conventions shall be as stated below, and shall be consistently applied across all productions:

FIELD NAME	FIELD DESCRIPTION
Begin Bates	The production Bates number associated with the first page of a Document.
End Bates	The production Bates number associated with the last page of a Document.
BeginFamily/BeginAttach	Begin Bates number of the first page of parent Document of family of attachments.
EndFamily/EndAttach	End Bates number of the last page of last attachment to a family of Documents.
AttachCount	Number of document attachments.
AttachNames	Native file names of each individual attachment, separated by semicolons.
Custodian	Identification of the custodian(s) from whom the file was sourced.
All Custodians	Identification of all custodians who the producing party agreed to produce and where a duplicate of the Document was de-duplicated when processing the documents.
File Path	The file path from which the document was collected
All Paths	Identification of all file paths for duplicate copies.
Author	Author field extracted from the Metadata of a Document or other creator identified for the Document.
From	From field extracted from the Metadata of an email message.
To	To field extracted from the Metadata of an email message.
Cc	Cc field extracted from the Metadata of an email message.
Bcc	Bcc field extracted from the Metadata of an email message.
Pages	Total number of pages in the Document.
Date Received	Datetime received (MM/DD/YYYY HH/MM/SS).
Date Sent	Datetime sent (MM/DD/YYYY HH/MM/SS).
Date Created	Datetime created (MM/DD/YYYY HH/MM/SS).
Date Modified	Datetime that a Document was last modified (MM/DD/YYYY HH/MM/SS).
Last Modified By	Identification of person(s) who last modified a Document.
Message Id	Unique Message Id.
In Reply To	Message ID of email that instant email is in reply to.

FIELD NAME	FIELD DESCRIPTION
Subject	Subject line extracted from an email, e-document or e-attachment.
Filename	The full name of the Native File.
File Extension	The extension of the file.
File Size	The size of the file in bytes.
MD5 Hash	The MD5 hash value of a Document.
SHA1 Hash	The SHA1 hash value of a Document.
NativePath	The relative path to the native file for this Document.
TextPath	The relative path to the text file for this Document.
Redacted	Whether a Document has redactions (Y/N).
Placeholder	Whether a Document has a placeholder image (Y/N).
Confidentiality	Level of Confidentiality assigned.
Track Changes	Document has track changes (Y/N).
Hidden Content	Identifies documents with hidden content (i.e. hidden rows, columns, sheets, or slides).
Speaker Notes	Document has speaker notes (Y/N).
Has Comments	Indicates there are comments in the document.
Production Volume	Production volume number (e.g., V001, V002, etc.).
Producing Party	Name of party producing the Document.

DATED: November 15, 2023

ORDER

Based on the foregoing, IT IS SO ORDERED.

Dated this 20th day of November, 2023.



Kymberly K. Evanson
United States District Judge